

United States Court of Appeals, Sixth Circuit.

Steven WARSHAK, Plaintiff-Appellee,
v.
UNITED STATES of America, Defendant-Appellant.

No. 06-4092.

Decided and Filed: June 18, 2007.

Before: MARTIN and DAUGHTREY, Circuit Judges; SCHWARZER, District Judge

OPINION

BOYCE F. MARTIN, JR., Circuit Judge.

The government appeals the district court's entry of a preliminary injunction, prohibiting it from seizing "the contents of any personal e-mail account maintained by an Internet Service Provider in the name of any resident of the Southern District of Ohio without providing the relevant account holder or subscriber prior notice and an opportunity to be heard on any complaint, motion, or other pleading seeking issuance of such an order." For the reasons discussed below, we largely affirm the district court's decision, requiring only that the preliminary injunction be slightly modified on remand.

I.

In March 2005, the United States was engaged in a criminal investigation of Plaintiff Steven Warshak and the company he owned, Berkeley Premium Nutraceuticals, Inc. The investigation pertained to allegations of mail and wire fraud, money laundering, and related federal offenses. On May 6, 2005, the government obtained an order from a United States Magistrate Judge in the Southern District of Ohio directing internet service provider ("ISP") NuVox Communications to turn over to government agents information pertaining to Warshak's e-mail account with NuVox. The infor-

mation to be disclosed included (1) customer account information, such as application information, "account identifiers," "[b]illing information to include bank account numbers," contact information, and "[any] other information pertaining to the customer, including set up, synchronization, etc."; (2) "[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled" by Warshak; and (3) "[a]ll Log files and backup tapes."

The order stated that it was issued under 18 U.S.C. § 2703, part of the Stored Communications Act ("SCA"), and that it was based on "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." The order was issued under seal, and prohibited NuVox from "disclos[ing] the existence of the Application or this Order of the Court, or the existence of this investigation, to the listed customer or to any person unless and until authorized to do so by the Court." The magistrate further ordered that "the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days." On September 12, 2005, the government obtained a nearly identical order pertaining to Yahoo, another ISP, that sought the same types of information from Warshak's Yahoo e-mail account and a Yahoo account identified with another individual named Ron Fricke.

On May 31, 2006, over a year after obtaining the NuVox order, the United States wrote to Warshak to notify him of both orders and their requirements.¹ The magistrate had unsealed both orders the previous day. Based on this disclosure, Warshak filed suit on June 12, 2006, seeking declaratory and injunctive relief, and alleging that

¹ The government has conceded that it violated the statute by waiting for over a year without providing notice of the e-mail seizures to Warshak or seeking extensions of the delayed notification period, and it appears to have violated the magistrate's decision for the same reason.

the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and the SCA. After filing the complaint, Warshak's counsel sought the government's assurance that it would not seek additional orders under section 2703(d) directed at his e-mails, at least for some discrete period of time during the pendency of his civil suit. The government declined to provide any such assurance. In response, Warshak moved for a temporary restraining order and/or a preliminary injunction prohibiting such future searches. The district court held a telephonic hearing on the motions, and eventually granted part of the equitable relief sought by Warshak.

In considering the factors for a preliminary injunction, the district court reasoned that e-mails held by an ISP were roughly analogous to sealed letters, in which the sender maintains an expectation of privacy. This privacy interest requires that law enforcement officials obtain a warrant, based on a showing of probable cause, as a prerequisite to a search of the e-mails. Because it viewed Warshak's constitutional claim as meritorious, the district court deemed it unnecessary to examine his likelihood of success on the SCA claim. . . .

[...]

The government appeals from the district court's ruling.

II.

[...]

III.

[...]

[The court recited the reasonable-expectation-of-privacy rule]. . . . [W]here the party challenging the disclosure has voluntarily disclosed his records to a third party, he maintains no expectation of privacy in the disclosure vis-à-vis that individual, and assumes the risk of that person disclosing (or being compelled to disclose) the shared information to the authorities. See, e.g., *United States v. Jacobsen*, 466 U.S. 109 (1984) (“[W]hen an individual reveals private information to another, he assumes the risk that his confidant will reveal that

information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information.”).

. . . . The government's . . . argument. . . begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-à-vis the party who is subject to compelled disclosure-in this instance, the ISPs. If he does not, . . . then the government must meet only the reasonableness standard applicable to compelled disclosures to obtain the material. If, on the other hand, the e-mail user does maintain a reasonable expectation of privacy in the content of the e-mails with respect to the ISP, then the Fourth Amendment's probable cause standard controls the e-mail seizure.

2. Reasonable expectation of privacy in e-mail content

Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, recognized by the Supreme Court in its line of cases involving government eavesdropping on telephone conversations. See *Smith v. Maryland*, 442 U.S. 735 (1979); *Katz v. United States*, 389 U.S. 347, (1967); *Berger v. New York*, 388 U.S. 41 (1967). In *Berger* and *Katz*, telephone surveillance that intercepted the content of a conversation was held to constitute a search, because the caller “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,” and therefore cannot be said to have forfeited his privacy right in the conversation. *Katz*, 389 U.S. at 352. This is so even though “[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.” *Smith*, 442 U.S. at 746 (Stewart, J., dissenting). On the other hand, in *Smith*, the Court ruled that the use of pen register, installed at the phone company's facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that “a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not

acquire the contents of communications.” 442 U.S. at 741.

. . . [T]he reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another. First, we must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded. Clearly, under *Katz*, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search. It is true, however, that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person. The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service’s ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company’s ability to access them.

The second necessary inquiry pertains to the precise information actually conveyed to the party through whom disclosure is sought or obtained. This distinction provides the obvious crux for the different results in *Katz* and *Smith*, because although the conduct of the telephone user in *Smith* “may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.” 442 U.S. at 743. [T]he caller in *Smith* “assumed the risk” of the phone company disclosing the records that he conveyed to it. Yet this assumption of the risk is limited to the specific information conveyed to the service provider, which in the telephone context excludes the content of the conversation. It is apparent, therefore, that although the government can

compel disclosure of a shared communication from the party with whom it was shared, it can only compel disclosure of the specific information to which the subject of its compulsion has been granted access. It cannot, on the other hand, bootstrap an intermediary’s limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).

This focus on the specific information shared with the subject of compelled disclosure applies with equal force in the e-mail context. Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber’s Fourth Amendment interest under *Smith*, because like the information obtained through the pen register in *Smith* and like the bank records in *Miller*, subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment. Consequently, the user does not maintain the same expectation of privacy in them vis-à-vis the service provider, and a third party subpoena to the service provider to access information that is shared with it likely creates no Fourth Amendment problems. The combined precedents of *Katz* and *Smith*, however, recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.

Similarly, under . . . *Katz*, if the government in this case had received the content of Warshak’s e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-à-vis his e-mailing partners. But this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents, much like the phone company in *Katz*. . . .

This analysis is consistent with other decisions that have addressed an individual's expectation of privacy in particular electronic communications. In *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001), we concluded that users of electronic bulletin boards lacked an expectation of privacy in material posted on the bulletin board, as such materials were "intended for publication or public posting." Of course the public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients. Although we stated that an e-mail sender would "lose a legitimate expectation of privacy in an e-mail that had already reached its recipient," analogizing such an e-mailer to "a letter-writer," this diminished privacy is only relevant with respect to the recipient, as the sender has assumed the risk of disclosure by or through the recipient. *Guest* did not hold that the mere use of an intermediary such as an ISP to send and receive e-mails amounted to a waiver of a legitimate expectation of privacy.

Other courts have addressed analogous situations where electronic communications were obtained based on the sender's use of a computer network. In *United States v. Simons*, the Fourth Circuit held that a government employee lacked a reasonable expectation of privacy in electronic files on his office computer, in light of the employer's policy that explicitly notified the employee of its intention to "audit, inspect, and monitor," his computer files. 206 F.3d 392, 398 (4th Cir. 2000). In light of this explicit policy, the employee's belief that his files were private was not objectively reasonable. On the other hand, in *United States v. Heckenkamp*, the Ninth Circuit held that a university student did have a reasonable expectation of privacy in his computer files even though he "attached [his computer] to the university network," because the "university policies do not eliminate Heckenkamp's expectation of privacy in his computer." 482 F.3d 1142, 1147 (9th Cir. 2007). Although the university did "establish limited instances in which university administrators may access his computer in order to protect the university's systems," this exception fell far short of a blanket

monitoring or auditing policy, and the Ninth Circuit deemed it insufficient to waive the user's expectation of privacy.

Heckenkamp and *Simons* provide useful bookends for the question before us, regarding when the use of some intermediary provider of computer and e-mail services—be it a commercial ISP, a university, an employer, or another type of entity—amounts to a waiver of the user's reasonable expectation of privacy in the content of the e-mails with respect to that intermediary. In instances where a user agreement explicitly provides that e-mails and other files will be monitored or audited as in *Simons*, the user's knowledge of this fact may well extinguish his reasonable expectation of privacy. Without such a statement, however, the service provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy, as in *Heckenkamp*.

Turning to the instant case, we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user "seeks to preserve as private," and therefore "may be constitutionally protected." *Katz*, 389 U.S. at 351. It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past.

The government asserts that ISPs have the contractual right to access users' e-mails. The district court's ruling was based on its willingness to credit Warshak's contrary factual argument that "employees of commercial ISPs [do not] open and read-[nor do] their subscribers reasonably expect them to open and read-individual subscriber e-mails as a matter of course." This factual determination tracks the language from [prior case law] that suggests a privacy interest in records held by a third party is

only undermined where the documents are accessed by the third party or its employees “in the ordinary course of business.” *Miller*, 425 U.S. at 442. Moreover, as explained in the Ninth Circuit’s decision in *Heckenkamp*, mere accessibility is not enough to waive an expectation of privacy. Where a user agreement calls for regular auditing, inspection, or monitoring of e-mails, the expectation may well be different, as the potential for an administrator to read the content of e-mails in the account should be apparent to the user. Where there is such an arrangement, compelled disclosure by means of an SCA order directed at the ISP would be akin to the third party subpoena directed at a bank, as in *Miller* and *Jerry T. O’Brien*. In contrast, the terms of service in question here, which the government has cited to in both the district court and this Court, clearly provide for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of e-mails.⁷ Because the ISPs right to access e-mails under these user agreements is reserved for extraordinary circumstances, much like the university policy in *Heckenkamp*, it is similarly insufficient to undermine a user’s expectation of privacy. For now, the government has made no showing that e-mail content is regularly accessed by ISPs, or that users are aware of such access of content.

The government also insists that ISPs regularly screen users’ e-mails for viruses, spam, and child pornography. Even assuming that this is true, however, such a process does not waive an expectation of privacy in the content of e-mails

⁷ See Gov’t Br. at 34 (citing Yahoo terms of service which allow access where “reasonably necessary to: (a) comply with legal process; (b) enforce the [Terms of Service]; (c) respond to claims that any Content violates the rights of third parties; (d) respond to your requests for customer service; or (e) protect the rights, property or personal safety of Yahoo!, its users and the public.”). As amicus Electronic Frontier Foundation points out, each instance involves outside prompting for an ISP to review content, and does not occur in the normal course of business. This type of accessibility by the service provider was rejected as diminishing the expectation of privacy in *Katz*, as well as in *Heckenkamp*.

sent through the ISP, for the same reasons that the terms of service are insufficient to waive privacy expectations. The government states that ISPs “are developing technology that will enable them to scan user images” for child pornography and viruses. The government’s statement that this process involves “technology,” rather than manual, human review, suggests that it involves a computer searching for particular terms, types of images, or similar indicia of wrongdoing that would not disclose the content of the e-mail to any person at the ISP or elsewhere, aside from the recipient. But the reasonable expectation of privacy of an e-mail user goes to the content of the e-mail message. The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual’s content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content. In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages. The fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send.

[...]

IV.

The district court correctly determined that e-mail users maintain a reasonable expectation of privacy in the content of their e-mails, and we agree that the injunctive relief it crafted was largely appropriate, although we find necessary one modification. . . .